Skew codes of prescribed distance or rank

Lionel Chaussade, Pierre Loidreau, Félix Ulmer

Skew codes of prescribed distance or rank

L. Chaussade*, P. Loidreau† and F. Ulmer ‡

March 17, 2008

Abstract

In this paper we propose two methods to produce block codes of prescribed rank or distance. Following [4, 5] we work with skew polynomial rings of automorphism type and the codes we investigate are ideals in quotients of this ring. There is a strong connection with linear difference operators and with linearized polynomials (or q-polynomials) reviewed in the first section.

1 Galois theory of difference equations over finite fields

A finite difference field $(\mathbb{F}_q, \theta)$ is a field together with an automorphism θ. A difference (or recurrence) equation over $(\mathbb{F}_q, \theta)$ is an equation of the form

$$L(y) \;=\; a_n\,\theta^n(y) + \;\ldots\; + \; a_1\theta(y) \;+\; a_0\,y \;=\; 0$$

Let $q = p^r$ and $\theta(x) = x^{p^i}$ with i in $\{0, ..., r-2\}$. A finite difference field $(\mathbb{F}_{q^s}, \Theta)$ is a difference field extension of $(\mathbb{F}_q, \theta)$ if $\mathbb{F}_q \subseteq \mathbb{F}_{q^s}$ and Θ defined by $\Theta(x) = x^{p^i}$ is an extension of θ to an automorphism of $\mathbb{F}_{q^s}$. Note that even if there are several ways to extend a field automorphism, we keep the expression θ for the extension Θ. A solution of the difference equation $L(y) = 0$ is an element β in a finite difference field extension of $(\mathbb{F}_q, \theta)$ such that $L(\beta) = 0$. We call $(\mathbb{F}_q)^\theta$ the field of constants. The solution space of the difference equation $L(y) = 0$ is a vector space over $(\mathbb{F}_q)^\theta$ of dimension $\leq n$. There is a difference Galois theory of difference rings [2, 14] where the existence of a difference splitting ring (of Picard-Vessiot ring) is proven under the assumption that the field of constants is algebraically closed. In our special situation of a finite coefficient field we do not want to work with an algebraically closed field of constants and we will show that if $a_0 \neq 0$, then a finite PV-field always exists. In connection with coding theory the equivalent notion of p-polynomial or linearized polynomial is more common ([10, 13]). In this section we recall the basic facts and connections between those notions.

*IRMAR (UMR 6625), Université de Rennes 1, Campus de Beaulieu, F-35042 Rennes Cedex
†IRMAR (UMR 6625) et DGA/CELAR, La Roche Marguerite, 35174 Bruz Cedex, France
‡IRMAR (UMR 6625), Université de Rennes 1, Campus de Beaulieu, F-35042 Rennes Cedex

To a difference equation $L(y)$ we can associate the corresponding difference operator $a_n\,\theta^n + \ldots + a_1\theta + a_0$. From the relation $\theta(a \cdot y) = \theta(a)\theta(y)$ we obtain the basic rule for the compositions of differential operators $\theta \cdot a = \theta(a) \cdot \theta$. To the difference operator $a_n\,\theta^n + \ldots + a_1\theta + a_0$ corresponding to $L(y)$ we associate the skew polynomial $f_L = a_nX^n + \ldots + a_1X + a_0 \in \mathbb{F}_q[X,\theta])$. Let us defines a ring structure on the set of skew polynomials

$$\mathbb{F}_q[X,\theta] \;=\; \left\{a_{n-1}X^{n-1} + \ldots + a_1X + a_0 \,|\, a_i \in \mathbb{F}_q \text{ and } n \in \mathbb{N}\right\}.$$

The addition in $\mathbb{F}_q[X,\theta]$ is defined to be the usual addition of polynomials and the multiplication is defined by the basic rule $Xa = \theta(a)X$ $(a \in \mathbb{F}_q)$ and extended to all elements of $\mathbb{F}_q[X,\theta]$ by associativity and distributivity (cf. [1, 12]). The non commutative multiplication of skew polynomials corresponds to the composition of differential operators. The ring $\mathbb{F}_q[X,\theta]$ is a left and right euclidean ring whose left and right ideals are principal [12]. Left and right gcd and lcm exist in $\mathbb{F}_q[X,\theta]$ and can be computed using the left and right euclidean algorithm [6]. Conversely we associate a difference equation $L_g(y)$ to a given skew polynomial $g \in \mathbb{F}_q[X,\theta]$.

Suppose that θ is defined as $a \mapsto a^{q_0}$. In this case $\mathbb{F}_{q_0} = (\mathbb{F}_q)^\theta$, where $(\mathbb{F}_q)^\theta$ is the fixed field $\mathbb{F}_q$ of θ. It is classical (Section 5 of [10] or "p-polynomials' in [13]) to associate to $L(y)$ the *linearized polynomial* :

$$\ell(Y) \;=\; a_n\,Y^{(q_0)^n} + \ldots + a_1Y^{q_0} + a_0\,Y \;\in \mathbb{F}_q[Y]. \tag{1}$$

This amounts to express the action of the automorphism, and therefore there is a bijective correspondance between solutions of $L(y) = 0$ in a finite difference field extension and distinct roots of the classical commutative polynomial $\ell(Y) = 0$.

Definition 1 *We call multiplicity of a solution, β, of $L(y) = 0$ the order of β as a root of the associated linearized polynomial $\ell(Y)$.*

Example 1 *In the previous example $L(y) = \theta^n(y)$, 0 is a solution of multiplicity $(q_0)^n$.*

The following is a reformulation of [10], Theorem 3.50:

Lemma 1 *Let θ be an automorphism of $\mathbb{F}_q$ defined by $a \mapsto a^{q_0}$, denote $(\mathbb{F}_q)^\theta = \mathbb{F}_{q_0}$ the fixed field of θ and $L(y) = \sum_{i=0}^n a_i\theta^i(y)$ with $a_i \in \mathbb{F}_q$. Each solution of $L(y) = 0$ has multiplicity $(q_0)^k$ where $k = \min\{i, a_i \neq 0\}$.*

Proof. The first part is proven in [10], Theorem 3.50 and only the claim on the dimension has to be verified. First we note that the derivative of $\ell(Y)$ is $\ell'(Y) = a_0$, so that if $a_0 \neq 0$ then all the solutions of $\ell(Y) = 0$ have multiplicity 1.
Suppose that $q = q_0^r$ and that $a_0 = a_1 = ... = a_{k-1} = 0$ and $a_k \neq 0$, then

$$\ell(Y) = \sum_{i=k}^{n} a_iY^{q_0^i} = \sum_{i=k}^{n} a_i^{q_0^{rk}}Y^{q_0^i}.$$

The last equality is true because a_i belongs to $\mathbb{F}_{q_0^r} = \mathbb{F}_q$. We get

$$\ell(Y) = \sum_{i=k}^{n} a_i^{q_0^{rk}} y^{q_0^i} = [\sum_{i=k}^{n} a_i^{q_0^{(r-1)k}} y^{q_0^{i-k}}]^{q_0^k}$$

By hypothesis the polynomial in brackets has a constant term $a_k^{q_0^{(r-1)k}} \neq 0$ and thus all its roots have order 1. Therefore all the solutions of $\ell(Y)$ have multiplicity q_0^k. ∎

The following theorem shows a link between the dimension of the vector space of solutions and the coefficients of L.

Theorem 1 *(cf. [13], Theorem 5) Let θ be an automorphism of $\mathbb{F}_q$ defined by $a \mapsto a^{q_0}$, denote $(\mathbb{F}_q)^\theta = \mathbb{F}_{q_0}$ the fixed field of θ and $L(y) = \sum_{i=0}^{n} a_i \theta^i(y)$ with $a_i \in \mathbb{F}_q$. There exists a finite field $\mathbb{F}_{q^s}$ which contains all the roots of $\ell_L(Y) = 0$ and the $(\mathbb{F}_q)^\theta$-subspace of $\mathbb{F}_{q^s}$ spanned by those roots is of dimension $n - \min\{i, a_i \neq 0\}$. In particular if $a_0 \neq 0$ then the smallest field $\mathbb{F}_{q^s}$ is a difference splitting field (or Picard-Vessiot field) of $L(y) = 0$.*

Proof. We compute the dimension of the vector space of solutions in a finite field extension by counting the solutions of the associated linearized polynomial $\ell(Y)$. Since $\ell(Y)$ is a polynomial of order q_0^n, it has q_0^n roots counted with multiplicity in a decomposition field. If $\min\{a_i,\ a_i \neq 0\} = k$ then the proof of lemma shows that $L(y)$ has q_0^n solutions of multiplicity q_0^k, it follows that the dimension of the vector space spanned by the solutions over $\mathbb{F}_{q_0}$ has dimension $n - k$. ∎

Example 2 *Let $\theta(x) = x^{q_0}$, then*

1. *The solution space of $L(y) = \theta^n(y) - y$ is $\mathbb{F}_{(q_0)^n}$. It is a vector space of dimension n over $\mathbb{F}_{q_0}$ (here $a_0 = 1 \neq 0$).*

2. *The solution space of $L(y) = \theta^n(y)$ is $\{0\}$. It is a vector space of dimension 0 ($a_0 = ...a_{n-1} = 0$ so $\min\{a_i,\ a_i \neq 0\} = n$).*

3. *The solution space of $L(y) = \theta^n(y) - \theta^{n-1}(y)$ is $\mathbb{F}_{q_0}$. To see this, note that if α is a solution, then $\theta(\alpha) - \alpha = 0$ and therefore $\alpha \in \mathbb{F}_{q_0}$. In this case the multiplicity of each solution is $(q_0)^{n-1}$.*

2 Skew codes with constructed rank

According to ([1], Theorem II.12), the two sided ideals of $\mathbb{F}_q[X, \theta]$ are generated by elements of the form $(b_0 + b_1 X^m + b_2 X^{2m} + \ldots + b_s X^{s \cdot m}) X^t$, where $m = | < \theta > |$ is the order of θ and $b_i \in (\mathbb{F}_q)^\theta$. The center $Z(\mathbb{F}_q[X, \theta])$ of $\mathbb{F}_q[X, \theta]$ is $(\mathbb{F}_q)^\theta[X^m]$. In particular a left or right ideal in $\mathbb{F}_q[X, \theta]$ generated by a central element is a two sided ideal. If I is a two sided ideal in $\mathbb{F}_q[X, \theta]$ then I is generated by a polynomial f of some degree n with the above property and, by the correspondance of ideals, the left ideals in $\mathbb{F}_q[X, \theta]/(f)$ are principal ideals,

each generated by a right divisor g of f. To the element $a(X) = a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ in $\mathbb{F}_q[X,\theta]/(f)$ we associate the word $a = (a_0, a_1, \ldots, a_{n-1}) \in \mathbb{F}_q^n$. The elements $a(X)$ of $\mathbb{F}_q[X,\theta]/(f)$ that belong to a left ideal in $\mathbb{F}_q[X,\theta]/(f)$ generated by a right divisor g of f form a linear $[n,k]$ code in $(\mathbb{F}_q)^n$, where $k = n - \deg(g)$. More precisely

Definition 2 *Let $f \in \mathbb{F}_q[X,\theta]$ be of degree n. If $I = (f)$ is a two sided ideal of $\mathbb{F}_q[X,\theta]$, then a θ-code $\mathcal{C}$ consists of code words $a = (a_0, a_1, \ldots, a_{n-1})$ that are coefficient tuples of elements $a(X) = a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ of a left ideal of $\mathbb{F}_q[X,\theta]/I$. In this case the elements $a(X)$ are left multiples of a right divisor g of f. We will focus on two special cases:*

1. *If $f \in Z(\mathbb{F}_q[X,\theta])$, then we call the θ-code corresponding to the left ideal $(g)/(f)$ a central θ-code.*
2. *If $m = |<\theta>|$ divides n and $f = X^n - 1$, then we call the θ-code corresponding to the left ideal $(g)/(X^n - 1)$ a θ-cyclic-code.*

Note that code words of skew codes can be identified with the multiples of the generating skew polynomial $g \in \mathbb{F}_q[X,\theta]$, but not with the solutions of the corresponding difference equations.

Any codeword of $(g)/(f)$ can be uniquely represented by a skew-polynomial of $\mathbb{F}_q[X,\theta]$ of degree $n-1$. Therefore it can be represented as a n-dimensional vector with components in $\mathbb{F}_q$. Since $[\mathbb{F}_q : (\mathbb{F}_q)^\theta] = m$, it can also be represented as a $m \times n$ matrix with coefficients over the field of constants. The rank of such a matrix is called the rank of the vector. It is clearly independent of the chosen basis of $\mathbb{F}_q/(\mathbb{F}_q)^\theta$

Definition 3 *The minimum rank distance of a code $\mathcal{C}$ of length n over $(\mathbb{F}_q)^\theta$ is the integer d such that*

$$d = \min_{c \in \mathcal{C} \setminus \{0\}} (Rk(c))$$

For a more precise description of rank metric in terms of coding theory, see [8].

Proposition 1 *Let $g \in \mathbb{F}_q[X,\theta]$ and $L_g(y) = 0$ be the associated differential equation. Suppose that there exists a solution β of $L_g(y) = 0$ in a finite difference field extension $\mathbb{F}_{q^s}$ and an integer $\delta \geq 1$ such that*

- *$\beta, \theta(\beta), \ldots, \theta^{n-1}(\beta)$ are linearly independent over $(\mathbb{F}_q)^\theta$.*
- *for $i \in \{0, \ldots, \delta-1\}$, the element $\theta^i(\beta)$ is a solution of $L_g(y) = 0$, i.e. $L_g(\theta^i(\beta)) = 0$.*

Then, for all skew polynomials f of degree n in the center of $\mathbb{F}_q[X,\theta]$ which are right divisible by g, the code $(g)/(f)$ has a minimum rank distance $\geq \delta + 1$. Therefore its minimum distance is at least $\delta + 1$.

PROOF. Let $c \in (g)/(f)$ be a non-zero codeword of rank t over $(\mathbb{F}_q)^\theta$. The coefficients of c form a n-dimensional vector $(c_0, \ldots, c_{n-1}) \in (\mathbb{F}_q)^n$ of rank t over $(\mathbb{F}_q)^\theta$. Hence, there exists $U \in M_{t\times n}((\mathbb{F}_q)^\theta)$ of rank t and $C_1, \ldots, C_t \in (\mathbb{F}_q)^t$ linearly independent over $(\mathbb{F}_q)^\theta$ such that

$$(c_0, \ldots, c_{n-1}) = (C_1, \ldots, C_t)U \tag{2}$$

Since a code word c is a left multiple $h \cdot g$ of g and since multiplication in $\mathbb{F}_q[X, \theta]$ corresponds to the composition of the differential operators, we have $L_c(y) = L_h(L_g(y))$. Therefore any solution γ of $L_g(y) = 0$ is also a solution of $L_c(y) = 0$ and there exists a basis of the space of solutions of the associated difference equation $L_g(y) = 0$ of the form $(\beta, \ldots, \theta^{\delta-1}(\beta), \gamma_\delta, \ldots, \gamma_{k-1})$. This shows that

$$(c_0, \ldots, c_{n-1}) \begin{pmatrix} \beta & \cdots & \theta^{\delta-1}(\beta) & \gamma_\delta & \ldots & \gamma_{k-1} \\ \theta(\beta) & \cdots & \theta^{\delta}(\beta) & \theta(\gamma_\delta) & \ldots & \theta(\gamma_{k-1}) \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \theta^{n-1}(\beta) & \cdots & \theta^{n+\delta-2}(\beta) & \theta^{n-1}(\gamma_\delta) & \ldots & \theta^{n-1}(\gamma_{k-1}) \end{pmatrix} = 0 \tag{3}$$

If we define

$$\forall i = 1, \ldots, t, \quad u_i(\beta) \stackrel{def}{=} \sum_{j=0}^{n} U_{ij}\theta^i(\beta),$$

and we replace $(c_0, \ldots, c_{n-1})$ by the expression (2), using the fact that the coefficients of U lie in the field of constants, we obtain

$$(C_1, \ldots, C_t) \begin{pmatrix} u_1(\beta) & \cdots & \theta^{\delta-1}(u_1(\beta)) & u_1(\gamma_\delta) & \ldots & u_1(\gamma_{k-1}) \\ u_2(\beta) & \cdots & \theta^{\delta-1}(u_2(\beta)) & u_2(\gamma_\delta) & \ldots & u_2(\gamma_{k-1}) \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ u_t(\beta) & \cdots & \theta^{\delta-1}(u_t(\beta)) & u_t(\gamma_\delta) & \ldots & u_t(\gamma_{k-1}) \end{pmatrix} = 0 \tag{4}$$

Since U has rank t, and since $\beta, \ldots, \theta^{N-1}(\beta)$ are linearly independent over the field of constants, this implies that $u_1(\beta), \ldots, u_t(\beta)$ are linearly independent over the field of constants and therefore the first δ columns of the matrix of the system are linearly independent. Hence if $t \leq \delta$, the previous equation has no non-zero solution. Therefore, the minimum rank distance of $(g)/(f)$ is at least $\delta + 1$. ∎

The above skew code of prescribed rank δ in the previous proposition will be denoted $\mathcal{C}_{\beta,\ldots,\theta^{\delta-1}(\beta)}$. In order to construct all codes $\mathcal{C}_{\beta,\ldots,\theta^{\delta-1}(\beta)}$ of length n, less than a given bound N, which are of prescribed rank δ defined over $\mathbb{F}_q$, we proceed as follows:

1. Consider in turn all non trivial automorphisms $\theta \in \mathrm{Aut}(\mathbb{F}_q)$. Trough this choice, the ring $\mathbb{F}_q[X, \theta]$ and therefore the constant field $(\mathbb{F}_q)^\theta$ of order q_0 are determined.

2. Consider in turn any β in a field extension $\mathbb{F}_{q^s}$ of $\mathbb{F}_q$ with $s \leq (q)^N$ (the degree of a linearized polynomial over $\mathbb{F}_q$ of some $f \in (\mathbb{F}_q)^\theta[X^{|\theta|}]$ of degree $n \leq N$). Compute the longest sequence $\beta, \theta(\beta), \ldots, \theta^t(\beta)$ in $\mathbb{F}_{q^s}$ that is linearly independent over $(\mathbb{F}_q)^\theta$.

Any subsequence $\beta, \ldots, \theta^{j-1}(\beta)$ could correspond to a $\mathcal{C}_{\beta,\ldots,\theta^{\delta-1}(\beta)}$ code, but we need to construct the code (the generating polynomial g having $\beta, \ldots, \theta^{\delta-1}(\beta)$ among its roots) in order to find δ and we need to verify that its length n (the degree of the bound of g) is less than t (we will see that the length n must in fact be t)

(a) Denote σ a generator of $\mathrm{Aut}(\mathbb{F}_{q^s}/\mathbb{F}_q)$. If σ is not a power of the extension of θ to $\Theta \in \mathrm{Aut}(\mathbb{F}_{q^s})$, then the fixed field of Θ is no longer contained in $\mathbb{F}_q$ and we stop the computation for this θ. Otherwise construct the smallest σ-invariant $(\mathbb{F}_q)^\theta$-subspace V_g of $\mathbb{F}_{q^s}$ containing $\beta, \ldots, \theta^{j-1}(\beta)$.

(b) Construct the skew polynomial $g \in \mathbb{F}_q[X, \theta]$ so that the corresponding difference operator $L_g(y) = 0$ has V_g as solution space. We will show that g is defined over $\mathbb{F}_q$ if and only if V_g is σ-invariant.

(c) Compute the bound $f \in (\mathbb{F}_q)^\theta[X^{|\theta|}]$ and verify that its degree n is less than t. In order to compute the bound f, we can use the algorithm described in the proof of ([5], Lemma 10). The computation of the bound will not be necessary, since we will show that g does generate a $\mathcal{C}_{\beta,\ldots,\theta^{\delta-1}(\beta)}$ code if and only the $(\mathbb{F}_q)^\theta$-subspace spanned by $\beta, \theta(\beta), \ldots, \theta^t(\beta)$ is the solution space of the difference operator corresponding to a central polynomial $f \in (\mathbb{F}_q)^\theta[X^{|\theta|}]$. Therefore we must have $n = t$.

Note that Gabidulin codes correspond to the case where the length n is maximal, i.e. $n = t = [\mathbb{F}_{q^s} : (\mathbb{F}_q)^\theta]$. In this case t is the order of $\mathrm{Aut}((\mathbb{F}_{q^s}/(\mathbb{F}_q)^\theta)$ and the bound f must be $X^t - 1$. We will be particularly interested in codes that are not of this type.

In the following we review the classical result showing how to reconstruct a difference equation from a given solution space or a fundamental set of solutions $\{y_1, \ldots, y_n\}$ (see [13], Theorem 7). This is always possible if $a_0 \neq 0$ and the case $a_0 = 0$ is less interesting since such a code is obtained from a code with $a_0 \neq 0$ by adding columns of zeros to the generating matrix ([5], Proposition 1). The solutions y of such a difference equation are precisely the y that are linearly dependent with $\{y_1, \ldots, y_n\}$, i.e. such that the Casoratian

$$\mathrm{Cas}(y_1, \ldots, y_n, y) = \begin{vmatrix} y_1 & y_2 & \ldots & y_n & y \\ \theta(y_1) & \theta(y_2) & \ldots & \theta(y_n) & \theta(y) \\ \theta^2(y_1) & \theta^2(y_2) & \ldots & \theta^2(y_n) & \theta^2(y) \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \theta^n(y_1) & \theta^n(y_2) & \ldots & \theta^n(y_n) & \theta^n(y) \end{vmatrix} = 0.$$

We denote by Cas_i the above determinant where the last column and the i-th row have been deleted. Expanding the determinant along the last column gives the

$$L_{y_1,\ldots,y_n}(y) = \theta^n(y) + \sum_{i=0}^{n-1} \frac{\mathrm{Cas}_{i+1}(y_1, \ldots, y_n, y)}{\mathrm{Cas}(y_1, \ldots, y_n)} \, \theta^i(y).$$

This allows to express the coefficients of a difference equation from a fundamental set of solutions and is therefore analogous to the result about symmetric functions. Next we want to insure that the code we are constructing is defined over $\mathbb{F}_q$.

Lemma 2 *Let $\theta \in Aut(\mathbb{F}_q)$, σ a generator of the Galois group of $\mathbb{F}_{q^s}/\mathbb{F}_q$ and $y_i \in \mathbb{F}_{q^s}$ such that $y_1, \cdots, y_n$ are linearly independent over $(\mathbb{F}_q)^\theta$. The difference equation $L_{y_1,\ldots,y_n}(y)$ is defined over $\mathbb{F}_q$ if and only if $y_1, \cdots, y_n$ span a $(\mathbb{F}_q)^\theta$-vector space that is invariant under σ.*

PROOF. In one direction we have to show that the coefficients of $L_{y_1,\ldots,y_n}(y)$ belong to $\mathbb{F}_q$:

$$\sigma\left(\frac{\mathrm{Cas}_{i+1}(y_1,\ldots,y_n,y)}{\mathrm{Cas}(y_1,\ldots,y_n)}\right) = \frac{\det(\sigma)\cdot \mathrm{Cas}_{i+1}(y_1,\ldots,y_n,y)}{\det(\sigma)\cdot \mathrm{Cas}(y_1,\ldots,y_n)} = \frac{\mathrm{Cas}_{i+1}(y_1,\ldots,y_n,y)}{\mathrm{Cas}(y_1,\ldots,y_n)}$$

and therefore the coefficients of $L_{y_1,\ldots,y_n}(y)$ belong to $\mathbb{F}_q$, the fixed field of σ. The proof of the above is similar to the differential case using the fact that σ and (the extension of) θ commute (cf. [15], p27, Exercice 4c).
For the converse, suppose that $L_{y_1,\ldots,y_n}(y) = \sum_{i=0}^n a_i\theta^i(y)$ with $a_i \in \mathbb{F}_q$. Since σ and (the extention to $\mathbb{F}_{q^s}$ of) θ commute, we get that

$$0 \;=\; \sigma\left(\sum_{i=0}^{n} a_i\theta^i(y_j)\right) \;=\; \sum_{i=0}^{n} a_i\theta^i(\sigma(y_j)),$$

which shows that the space spanned by $y_1, \cdots, y_n$ is invariant under σ. ∎

We are now in a position to compute the smallest generating polynomial g having the roots $\beta, \theta(\beta), \ldots, \theta^{\delta-1}(\beta)$ and to guarantee that it is defined over $\mathbb{F}_q$. For that we consider a basis $y_1, \ldots, y_\ell$ of the space spanned by $\beta, \theta(\beta), \ldots, \theta^{\delta-1}(\beta)$. We add to this set of linearly independent vectors any image under the generators σ of $\mathrm{Aut}(\mathbb{F}_{q^s}/\mathbb{F}_q)$ of the basis vectors, until we obtain a basis $y_1, \ldots, y_r$ that is stable under σ. According to the above Lemma, the corresponding difference equation $L_{y_1,\ldots,y_r}(y)$ is defined over $\mathbb{F}_q$ and has the solutions $\beta, \theta(\beta), \ldots, \theta^{\delta-1}(\beta)$.

We now focus on the length of the code generated by the skew polynomial g corresponding to the difference operator $L_{y_1,\ldots,y_r}(y)$. According to ([5], Definition 1), we need a two sided ideal (f) contained in the left ideal $(g) \subset \mathbb{F}_q[X,\theta]$ in order to determine the length of the code $(g)/(f)$ (i.e. the number of columns of the generating matrix). Such a skew polynomial f must belong to $(\mathbb{F}_q)^\theta[X^{|\theta|}]$, the center of $\mathbb{F}_q[X,\theta]$, and is called a bound for g. An algorithm to find f from g is described in ([5], Lemma 4). In our special situation, according to the above definition of a skew code of prescribed rank, we also need f to be of degree at most n, where n is the largest integer such that the elements $\beta, \theta(\beta), \ldots, \theta^{n-1}(\beta)$ of $\mathbb{F}_{q^s}$ are linearly independent over the fixed field $(\mathbb{F}_q)^\theta$. We now show that f must be $L_{\beta,\theta(\beta),\ldots,\theta^{n-1}(\beta)}(y)$, therefore in the algorithm we will just need to test that the differential operator corresponding to $L_{\beta,\theta(\beta),\ldots,\theta^{n-1}(\beta)}(y)$ belongs to $(\mathbb{F}_q)^\theta[X^{|\theta|}]$. To see this, note if $f = h \cdot g \in (\mathbb{F}_q)^\theta[X^{|\theta|}]$, then by division in $\mathbb{F}_{q^s}[X,\theta]$ we have $f = q_\beta \cdot (X-\beta) + r_\beta$ with $r_\beta \in \mathbb{F}_{q^s}$, therefore r_β must be zero. Since the application $\phi\colon \mathbb{F}_4[X,\theta] \to \mathbb{F}_4[X,\theta]$ defined by $\phi(\sum_{i=0}^n a_iX^i) = \sum_{i=0}^n \theta(a_i)X^i$ is a morphism ([5], proof of Lemma 21), we have that $f = q_{\theta^i(\beta)} \cdot (X - \theta^i(\beta))$ for $i \in \{1, \ldots, n-1\}$. This shows that the degree of f is at least n and that if the degree is n, then the solution space of f is spanned by $\beta, \theta(\beta), \ldots, \theta^{n-1}(\beta)$.

This proves the claim and leads to the following algorithm to construct all code $\mathcal{C}_{\beta,\ldots,\theta^{\delta-1}(\beta)}$ of length n less than a given bound N which are of prescribed rank $\delta \geq \Delta$ defined over $\mathbb{F}_q$, we proceed as follows:

1. Consider in turn all non trivial automorphisms $\theta \in \mathrm{Aut}(\mathbb{F}_q)$. At this point we fixed the ring $\mathbb{F}_q[X,\theta]$ and therefore the constant field $(\mathbb{F}_q)^\theta$ of order q_0.

2. Consider in turn any β in a field extension $\mathbb{F}_{q^s}$ of $\mathbb{F}_q$ with $s \leq (q)^N$ with the property that a generator σ of $\mathrm{Aut}(\mathbb{F}_{q^s}/\mathbb{F}_q)$ is a power of the extension of θ to $\Theta \in \mathrm{Aut}(\mathbb{F}_q^s)$.

3. For each β compute the longest sequence $\beta, \theta(\beta), \ldots, \theta^{n-1}(\beta)$ in $\mathbb{F}_{q^s}$ that is linearly independent over $(\mathbb{F}_q)^\theta$ and check that f corresponding to $L_{\beta,\theta(\beta),\ldots,\theta^{n-1}(\beta)}(y)$, which by construction belongs to $f \in (\mathbb{F}_q)^\theta[X,\theta]$, is central, i.e. belongs to $(\mathbb{F}_q)^\theta[X^{|\theta|}]$.

4. If $f \in (\mathbb{F}_q)^\theta[X^{|\theta|}]$, then for any subsequence $\beta, \ldots, \theta^{j-1}(\beta)$, construct the smallest σ-invariant $(\mathbb{F}_q)^\theta$-subspace V_j of $\mathbb{F}_{q^s}$ containing $\beta, \ldots, \theta^{j-1}(\beta)$, where σ is a the generator of $\mathrm{Aut}(\mathbb{F}_{q^s}/\mathbb{F}_q)$. It is sufficient to iteratively add the image of a basis under σ that is not linearly dependent with the space constructed so far, until no such image appears.

5. The resulting skew polynomial $g \in \mathbb{F}_q[X,\theta]$ will be a skew code of prescribed rank δ, where δ is the largest integer such that $\{\beta, \ldots, \theta^{\delta-1}(\beta)\} \subset V_j$.

Example 3 *Consider $\mathbb{F}_q = \mathbb{F}_4$, $\theta(x) = x^2$ and $s = 6$. This means that we will use elements $\beta \in \mathbb{F}_{4^6}$ in order to construct codes over $\mathbb{F}_4$. We denote by α the generator of $\mathbb{F}_{4^6}$ and w the generator of $\mathbb{F}_4$ given by* Magma.

1. *Consider $\beta = \alpha^{3688}$. The longest sequence which is linearly independent over $\mathbb{F}_2 = (\mathbb{F}_4)^\theta$ is $\beta, \theta(\beta), \ldots, \theta^7(\beta)$. Therefore, if we obtain a skew code of constructed rank, this code must be of length $n = 8$. Using the Casoratian determinant we compute $L_\beta(y) = (\theta^8 + \theta^6 + \theta^2 + 1)(y)$. Since the associated operator $f_L = X^8 + X^6 + X^2 + 1 \in \mathbb{F}_2[X,\theta]$ is a central polynomial (i.e. $f \in \mathbb{F}_2[X^2]$), we will be able to construct a skew code over $\mathbb{F}_4$ of constructed rank using this $\beta \in \mathbb{F}_{4^6}$. We start with $j = 1$, and compute the smallest $\mathbb{F}_2$-space V_1 containing $\{\beta\}$ which is stable under the generator $\sigma\colon x \mapsto x^4$ of $Aut(\mathbb{F}_{4^6}/\mathbb{F}_4)$. A basis of V_1 is $\{\beta, \theta^2(\beta), \theta^4(\beta), \theta^6(\beta)\}$ (note that $\sigma = \theta^2$). Using the Casoratian determinant, we compute the skew polynomial $g = X^4 + \alpha^{2730}X^3 + X^2 + X + 1 = X^4 + wX^3 + X^2 + X + 1$ associated with the corresponding difference operator having the solution space V_1. Since the length of the skew code is 4, its generating matrix is*

$$\begin{pmatrix} 1 & 1 & 1 & w^2 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & w & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & w^2 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & w & 1 \end{pmatrix}$$

We obtain a $[8,4,4]$ skew code over $\mathbb{F}_4$ of prescribed rank 2. This code maps to a $[16,8,4]$ code over $\mathbb{F}_2$.

2. *Consider* $\beta = \alpha^{1444}$. *The longest sequence which is linearly independent over* $\mathbb{F}_2 = (\mathbb{F}_4)^\theta$ *is* $\beta, \theta(\beta), \ldots, \theta^{11}(\beta)$. *This means that* β *generates a normal basis and that the bound must be* $f = X^{12} - 1$ *(which is always a bound in this case, because the order of* $\theta \in Aut(\mathbb{F}_{4^6}/\mathbb{F}_2)$ *is* 12*). The resulting code will be a Gabidulin code. The smallest* $\mathbb{F}_2$*-space* V_1 *containing* $\{\beta\}$ *which is stable under the generator* $\sigma\colon x \mapsto x^4$ *of* $Aut(\mathbb{F}_{4^6}/\mathbb{F}_4)$ *has basis* $\{\beta, \theta^2(\beta), \theta^4(\beta), \theta^6(\beta), \theta^8(\beta), \theta^{10}(\beta)\}$. *Using the Casoratian determinant, we compute the skew polynomial*

$$\begin{aligned} g &= X^6 + \alpha^{1365}X^5 + \alpha^{1365}X^4 + \alpha^{1365}X^3 + \alpha^{2730}X^2 + \alpha^{1365}X + 1 \\ &= X^6 + w^2X^5 + w^2X^4 + w^2X^3 + wX^2 + w^2X + 1. \end{aligned}$$

Since the length of the skew code is 12*, its generating matrix is*

$$\begin{pmatrix} 1 & w^2 & w & w^2 & w^2 & w^2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & w & w^2 & w & w & w & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & w^2 & w & w^2 & w^2 & w^2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & w & w^2 & w & w & w & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & w^2 & w & w^2 & w^2 & w^2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & w & w^2 & w & w & w & 1 \end{pmatrix}$$

We obtain a $[12, 6, 6]$ *skew code over* $\mathbb{F}_4$ *of prescribed rank* 2 *which is a Gabidulin code. This code maps to a* $[24, 12, 6]$ *code over* $\mathbb{F}_2$.

Example 4 *Consider* $\mathbb{F}_q = \mathbb{F}_{2^4} = \mathbb{F}_{16}$, $\theta(x) = x^4$ *and* $s = 4$. *This means that we will use elements* $\beta \in \mathbb{F}_{2^{16}}$ *in order to construct codes over* $\mathbb{F}_{2^4}$. *We denote by* α *the generator of* $\mathbb{F}_{2^{16}}$ *and* w *the generator of* $\mathbb{F}_{2^4}$ *given by* MAGMA.

1. *Consider* $\beta = \alpha^{57153}$. *The longest sequence which is linearly independent over* $\mathbb{F}_{2^2} = (\mathbb{F}_{2^4})^\theta$ *is* $\beta, \theta(\beta), \ldots, \theta^7(\beta)$. *Therefore, if we obtain a skew code of constructed rank, this code must be of length* $n = 8$. *Using the Casoratian determinant we compute* $L_\beta(y) = (\theta^8 - 1)(y)$. *Since the associated operator* $f_L = X^8 - 1 \in \mathbb{F}_{2^2}[X, \theta]$ *is a central polynomial (i.e.* $f \in \mathbb{F}_{2^2}[X^4]$*), we will be able to construct a skew code over* $\mathbb{F}_{2^4}$ *of constructed rank using this* $\beta \in \mathbb{F}_{2^{16}}$. *We start with* $j = 1$*, and compute the smallest* $\mathbb{F}_2$*-space* V_1 *containing* $\{\beta\}$ *which is stable under the generator* $\sigma\colon x \mapsto x^{16}$ *of* $Aut(\mathbb{F}_{2^{16}}/\mathbb{F}_{16})$. *A basis of* V_1 *is* $\{\beta, \theta^2(\beta), \theta^4(\beta), \theta^6(\beta), \}$ *(note that* $\sigma = \theta^2$*). Using the Casoratian determinant, we compute the skew polynomial*

$$\begin{aligned} g &= X^4 + \alpha^{17476}X^3 + \alpha^{56797}X^2 + \alpha^{39321}X + \alpha^{39321} \\ &= X^4 + w^4X^3 + w^{13}X^2 + w^9X + w^9 \end{aligned}$$

associated with the corresponding difference operator having the solution space V_1. *Since the length of the skew code is* 4*, its generating matrix is*

$$\begin{pmatrix} w^9 & w^9 & w^{13} & w^4 & 1 & 0 & 0 & 0 \\ 0 & w^6 & w^6 & w^7 & w & 1 & 0 & 0 \\ 0 & 0 & w^9 & w^{13} & w^4 & 1 & 0 & \\ 0 & 0 & 0 & w^6 & w^6 & w^7 & w & 1 \end{pmatrix}$$

We obtain a $[8,4,5]$ *skew code over* $\mathbb{F}_{16}$ *of prescribed rank* 2 *which is a Gabidulin code. This code maps to a* $[32,16,7]$ *code over* $\mathbb{F}_2$.

2. $\beta = \alpha^{57153}$. *The longest sequence which is linearly independent over* $\mathbb{F}_{2^2} = (\mathbb{F}_{2^4})^\theta$ *is* $\beta, ..., \theta^5(\beta)$. *Therefore, if we obtain a skew code of constructed rank, this code must be of length* $n = 6$. *Using the Casoratian determinant we compute* $L_\beta(y) = (\theta^6+\theta^4+\theta^2+1)(y)$. *Since the associated operator* $f_L = X^6+X^4+X^2+1 \in \mathbb{F}_{2^2}[X,\theta]$ *is a central polynomial (i.e.* $f \in \mathbb{F}_{2^2}[X^4]$*), we will be able to construct a skew code over* $\mathbb{F}_{2^4}$ *of constructed rank using this* $\beta \in \mathbb{F}_{2^{16}}$. *A basis of* V_1 *is* $\{\beta, \theta^2(\beta), \theta^4(\beta), \}$ *(note that* $\sigma = \theta^2$*). Using the Casoratian determinant, we compute the skew polynomial*

$$\begin{aligned} g &= X^3 + \alpha^{61166}X^2 + \alpha^{56797}X + 1 \\ &= X^3 + w^{14}X^2 + w^{13}X + 1 \end{aligned}$$

associated to the corresponding difference operator having the solution space V_1. *Since the length of the skew code is* 4, *its generating matrix is*

$$\begin{pmatrix} 1 & w^{13} & w^{14} & 1 & 0 & 0 \\ 0 & 1 & w^7 & w^{11} & 1 & 0 \\ 0 & 0 & 1 & w^{13} & w^{14} & 1 \end{pmatrix}$$

We obtain a $[6,3,4]$ *skew code over* $\mathbb{F}_{16}$ *of prescribed rank* 2 *which is not a Gabidulin code.*

The following table shows the characteristics of codes with prescribed rank that are defined over $\mathbb{F}_4$. The lines indicate the fields where β has been found and the columns indicate the rank δ that has been prescribed during the construction (the actual prescribed distance could be larger). The entry $[10,5,4](8)$ means that 8 different skew polynomials g have been found that lead to a $[10,5,4]$ code. We also indicate a Gabidulin code with an index g. Note that codes with the same properties can be obtained using elements β in very different extensions. In the tables we only included those β that do not belong to any subfield. In all the examples that follow, imposing a certain rank never results in a code having a higher rank.

	$\delta = 1$
$\mathbb{F}_4$	$[\mathbf{2},\mathbf{1},\mathbf{2}]_g(2)$
$\mathbb{F}_{4^2}$	$[\mathbf{4},\mathbf{2},\mathbf{3}]_g(4)$
$\mathbb{F}_{4^3}$	$[6,3,2]_g(2)$ $[6,3,3]_g(4)$ $[\mathbf{6},\mathbf{3},\mathbf{4}]_g(2)$ $[\mathbf{4},\mathbf{2},\mathbf{2}](4)$
$\mathbb{F}_{4^4}$	$[\mathbf{8},\mathbf{4},\mathbf{4}]_g(16)$ $[\mathbf{6},\mathbf{3},\mathbf{3}](8)$
$\mathbb{F}_{4^5}$	$[10,5,2]_g(2)$ $[10,5,4]_g(14)$ $[\mathbf{10},\mathbf{5},\mathbf{5}]_g(16)$ $[8,4,2](2)$ $[8,4,3](2)$ $[\mathbf{8},\mathbf{4},\mathbf{4}](12)$

	$\delta = 1$
$\mathbb{F}_{4^6}$	$[12,6,3]_g(12)$ $[12,6,4]_g(12)$ $[12,6,5]_g(32)$ $[\mathbf{12},\mathbf{6},\mathbf{6}]_g(8)$ $[10,5,3]$ $[\mathbf{10},\mathbf{5},\mathbf{4}](8)$ $[8,4,2](2)$ $[8,4,3](8)$ $[\mathbf{8},\mathbf{4},\mathbf{4}](22)$

	$\delta = 1$
$\mathbb{F}_{4^7}$	$[14,7,2]_g(2)$ $[14,7,4]_g(14)$ $[14,7,5]_g(40)$ $[\mathbf{14},\mathbf{7},\mathbf{6}]_g(72)$ $[12,6,2](2)$ $[12,6,4](30)$ $[\mathbf{12},\mathbf{6},\mathbf{5}](32)$ $[8,4,2](4)$ $[8,4,3](24)$ $[\mathbf{8},\mathbf{4},\mathbf{4}](4)$ $[\mathbf{6},\mathbf{3},\mathbf{3}](16)$

The following tables, organized in the same way as the previous tables, show the characteristics of codes with prescribed rank that are defined over $\mathbb{F}_8$.

	$\delta = 1$	$\delta = 2$
$\mathbb{F}_8$	$[\mathbf{3},\mathbf{2},\mathbf{2}]_g(3)$	$[\mathbf{3},\mathbf{1},\mathbf{3}]_g(3)$
$\mathbb{F}_{8^2}$	$[6,4,2]_g(3)$ $[\mathbf{6},\mathbf{4},\mathbf{3}]_g(9)$	$[6,2,3]_g(3)$ $[\mathbf{6},\mathbf{2},\mathbf{5}]_g(9)$
$\mathbb{F}_{8^3}$	$[9,6,3]_g(54)$ $[\mathbf{9},\mathbf{6},\mathbf{4}]_g(9)$ $[\mathbf{6},\mathbf{4},\mathbf{3}](21)$	$[9,3,6]_g(54)$ $[\mathbf{9},\mathbf{3},\mathbf{7}]_g(9)$ $[\mathbf{6},\mathbf{2},\mathbf{5}](21)$
$\mathbb{F}_{8^4}$	$[12,8,2]_g(3)$ $[12,8,3]_g(63)$ $[\mathbf{12},\mathbf{8},\mathbf{4}]_g(126)$ $[9,6,2](3)$ $[\mathbf{9},\mathbf{6},\mathbf{3}](45)$	$[12,4,3]_g(3)$ $[12,4,5]_g(9)$ $[12,4,6]_g(54)$ $[12,4,7]_g(54)$ $[\mathbf{12},\mathbf{4},\mathbf{8}]_g(72)$ $[9,3,3](3)$ $[9,3,5](9)$ $[\mathbf{9},\mathbf{3},\mathbf{6}](36)$

	$\delta = 1$	$\delta = 2$
$\mathbb{F}_{8^5}$	$[15,10,2]_g(5)$ $[15,10,3]_g(120)$ $[15,10,4]_g(432)$ $[\mathbf{15},\mathbf{10},\mathbf{5}]_g(120)$ $[12,8,2](3)$ $[12,8,3](78)$ $[\mathbf{12},\mathbf{8},\mathbf{4}](144)$	$[15,5,3]_g$ $[15,5,6]_g$ $[15,5,7]_g$ $[15,5,8]_g$ $[\mathbf{15},\mathbf{5},\mathbf{9}]_g$ $[12,4,3]$ $[12,4,5]$ $[12,4,6]$ $[\mathbf{12},\mathbf{4},\mathbf{7}]$

The following tables, organized in the same way as the previous tables, show the characteristics of codes with prescribed rank that are defined over $\mathbb{F}_{16}$.

	$\delta = 1$	$\delta = 2$	$\delta = 3$
$\mathbb{F}_{16}$	$[\mathbf{4}, \mathbf{3}, \mathbf{2}]_g(8)$	$[\mathbf{4}, \mathbf{2}, \mathbf{3}]_g(8)$	$[\mathbf{4}, \mathbf{1}, \mathbf{4}]_g(8)$
$\mathbb{F}_{16^2}$	$[\mathbf{8}, \mathbf{6}, \mathbf{3}]_g(64)$	$[8, 4, 4]_g(32)$ $[\mathbf{8}, \mathbf{4}, \mathbf{5}]_g(32)$	$[\mathbf{8}, \mathbf{2}, \mathbf{7}]_g(64)$
$\mathbb{F}_{16^3}$	$[12, 9, 2]_g(32)$ $[12, 9, 3]_g(408)$ $[\mathbf{12}, \mathbf{9}, \mathbf{4}]_g(72)$ $[8, 6, 2](16)$ $[\mathbf{8}, \mathbf{6}, \mathbf{3}](48)$	$[12, 6, 3]_g(8)$ $[12, 6, 4]_g(72)$ $[12, 6, 5]_g(136)$ $[\mathbf{12}, \mathbf{6}, \mathbf{6}]_g(296)$ $[8, 4, 3](16)$ $[8, 4, 4](40)$ $[\mathbf{8}, \mathbf{4}, \mathbf{5}](8)$	$[12, 3, 4]_g(8)$ $[12, 3, 6]_g(64)$ $[12, 3, 8]_g(152)$ $[12, 3, 9]_g(216)$ $[\mathbf{12}, \mathbf{3}, \mathbf{10}]_g(72)$ $[8, 2, 4](8)$ $[8, 2, 5](8)$ $[\mathbf{8}, \mathbf{2}, \mathbf{7}](48)$
$\mathbb{F}_{16^4}$	$[16, 12, 3]_g(256)$ $[16, 12, 4]_g(3840)$ $[\mathbf{12}, \mathbf{9}, \mathbf{3}](512)$	$[16, 8, 6]_g(368)$ $[16, 8, 7]_g(3008)$ $[\mathbf{16}, \mathbf{8}, \mathbf{8}]_g(720)$ $[12, 6, 5](192)$ $[\mathbf{12}, \mathbf{6}, \mathbf{6}](320)$	$[16, 4, 10]_g(256)$ $[16, 4, 11]_g(1536)$ $[\mathbf{16}, \mathbf{4}, \mathbf{12}]_g(2304)$ $[\mathbf{12}, \mathbf{3}, \mathbf{8}](512)$

Example 5 *Using elements in $\mathbb{F}_{8^8}$, we found the following codes $[21, 14, 6]$ (best know distance) defined over $\mathbb{F}_8$:*

1. *The code generated by*

$$g = X^7 + wX^6 + w^3X^5 + w^5X^4 + w^6X^3 + w^4X^2 + w \in \mathbb{F}_8[X, \theta]$$

where w the generator of $\mathbb{F}_8$ given by Magma. *The bound of g is $f = X^{21} + X^{18} + X^{15} + X^{12} + X^9 + X^6 + X^3 + 1 \in \mathbb{F}_2[X^3]$. This code is not a Gabidulin code.*

2. *The code generated by*

$$g = X^7 + wX^6 + w^3X^5 + w^4X^4 + w^5X^3 + w^3X^2 + wX + w^2 \in \mathbb{F}_8[X, \theta]$$

where w the generator of $\mathbb{F}_8$ given by Magma. *The bound of g is $f = X^{21} + 1 \in \mathbb{F}_2[X^3]$. According to his bound, this code is a Gabidulin code.*

3 Skew codes with constructed distance

In the previous section we worked with solutions of linear difference equations, while in this section we will consider (right) *roots* of the associated skew polynomial.

Definition 4 *$\alpha \in \mathbb{F}_{q^s}$ is a root of skew polynomial $f \in \mathbb{F}_q[X, \theta]$ if and only if f is right divisible by $X - \alpha$.*

These codes are built in analogy to BCH codes and in the next section we adapt the classical algorithm for BCH to decode them.

As for linear difference equations, it is possible to find the roots of a skew polynomial by solving an associated commutative polynomial. Following [9], for $\alpha \in \mathbb{F}_{q^s}$ and $\theta \in Aut(\mathbb{F}_{q^s})$ we denote $\mathcal{N}_{\theta,i}(\alpha) = \theta^{i-1}(\alpha)\cdots\theta(\alpha)\cdot\alpha$. From [9] Theorem 1.3.11 we get that $a_nX^n + \ldots + a_1X + a_0 \in \mathbb{F}_q[X,\theta]$ is right divisible by $X-\alpha$ if and only if α is a zero of the associated polynomial

$$\mathcal{P}_f \;=\; \sum_{i=0}^{n} a_i \mathcal{N}_{\theta,n-i}(Y) \;\in \mathbb{F}_q[Y].$$

If θ is defined by $a \mapsto a^{q_0}$, this corresponds to

$$\begin{aligned}\mathcal{P}_f &= \sum_{i=0}^{n} a_i Y^{(q_0)^{i-1}+(q_0)^{i-2}+\ldots+1} \\ &= \sum_{i=0}^{n} a_i Y^{\frac{(q_0)^i-1}{q_0-1}} \;\in \mathbb{F}_q[Y]\end{aligned}$$

The following Lemma show the link between roots of skew polynomials and solutions of the associated difference equation:

Lemma 3 *Let θ be an automorphism of $\mathbb{F}_q$, $L(y) = \sum_{i=0}^{n} a_i\,\theta^i(y)$ a difference equation and $P = \sum_{i=0}^{n} a_iX^i$ the corresponding operator in $\mathbb{F}_q[X,\theta]$. Then a non zero element β of $\mathbb{F}_{q^s}$ is a solution of $L(y)=0$ if and only if $X - \frac{\theta(\beta)}{\beta}$ is a right divisor of P_L in $\mathbb{F}_{q^s}[X,\theta]$.*

Proof. Suppose that $L(\beta) = 0$. Using the right euclidean algorithm we obtain $P_L = Q\cdot(X-\frac{\theta(\beta)}{\beta}) + R$ where $R \in \mathbb{F}_q$. Since β is a solution of $(\theta - \frac{\theta(\beta)}{\beta})(y) = 0$, we obtain $0 = L(\beta) = P_L(\beta) = R\cdot\beta$, showing that $R = 0$. Conversely if $R = 0$ then $X - \frac{\theta(\beta)}{\beta}$ is a right factor of P_L, showing that $L(\alpha) = 0$. ∎

Lemma 4 *Let $\theta \in Aut(\mathbb{F}_q)$ be defined by $a \mapsto a^{q_0}$ and $\mathbb{F}_{q_0} = (\mathbb{F}_q)^\theta$ be the fixed field of θ in $\mathbb{F}_q$. If $\mathbb{F}_q \subset \mathbb{F}_{q^s}$ is an extension of finite fields and $\theta \in Aut(\mathbb{F}_q/(\mathbb{F}_q)^\theta)$, then for any σ in $Aut(\mathbb{F}_{q^s}/\mathbb{F}_q)$ the map*

$$\begin{aligned}\varphi_\sigma\colon \mathbb{F}_{q^s}[X,\theta] &\to \mathbb{F}_{q^s}[X,\theta] \\ \sum_{i=0}^{n} a_iX^i &\mapsto \sum_{i=0}^{n} \sigma(a_i)X^i\end{aligned}$$

is a morphism of rings.

Proof. we denote again θ the extension of the automorphism

$$\begin{aligned}\theta\colon \mathbb{F}_q &\to \mathbb{F}_q \\ a &\mapsto a^{q_0}\end{aligned}$$

to $\mathbb{F}_{q^s}$. Since addition in $\mathbb{F}_{q^s}[X,\theta]$ is the same as in $\mathbb{F}_{q^s}[X]$ and since $\sigma\colon \mathbb{F}_{q^s} \to \mathbb{F}_{q^s}$ can be extended to a morphism of $\mathbb{F}_q[X]$ by $X \mapsto X$, we get that φ_σ is a morphism of the additive group $(\mathbb{F}_{q^m}[X,\theta],+)$. For the mutiplication we have $\varphi_\sigma(aX) = \varphi_\sigma(a)\varphi_\sigma(X)$, but we also need $\varphi_\sigma(Xa) = \varphi_\sigma(X)\varphi_\sigma(a)$, or equivalently

$$\sigma(\theta(a))X = \varphi_\sigma(\theta(a)X) = \varphi_\sigma(Xa) = \varphi_\sigma(X)\varphi_\sigma(a) = \theta(\sigma(a))X.$$

The condition turns out to be $\theta\sigma = \sigma\theta$. The later is true because $\mathrm{Aut}(\mathbb{F}_{q^s}/(\mathbb{F}_{q^s})^\theta)$ is cyclic and σ is a power of the generator of $\mathrm{Aut}(\mathbb{F}_{q^s}/(\mathbb{F}_{q^s})^\theta)$. ∎

Lemma 5 *Let $f = a_nX^n + \ldots + a_1X + a_0 \in \mathbb{F}_q[X,\theta]$ and assume that $a_0 \neq 0$, then there is a finite field extension $\mathbb{F}_{q^s}$ such that f is the least common left multiple of polynomials $X - \alpha_i$, where $\alpha_i \in \mathbb{F}_{q^s}$.*

Proof. Since $a_0 \neq 0$, Theorem 1 shows that a finite splitting field exists for $f(y) = 0$. For any solutions $\beta \in \mathbb{F}_{q^s}$ of $f(y) = 0$, we have that $X - \frac{\theta(\beta)}{\beta}$ is a right factor of f in $\mathbb{F}_{q^s}[X,\theta]$. Therefore the least common left multiple g of the $X - \frac{\theta(\beta)}{\beta}$, where β runs over all the solutions of $f(y) = 0$ is also a right factor of f. Let σ be a generator of $\mathrm{Aut}(\mathbb{F}_{q^s}/\mathbb{F}_q)$, then σ commutes with the extension of θ to $\mathbb{F}_{q^s}$ and therefore maps a solution of $f(y) = 0$ into another solution. This shows that φ_σ maps g to itself and therefore g is defined over $\mathbb{F}_q$. Since all solutions of f are solutions of g, the degree of g must be the same as the degree of f, which show that they coincide. ∎

In analogy to BCH codes, skew BCH codes with designed distance are introduced in [4] in the case where q is a power of 2. We now extend this definition to an arbitrary field $\mathbb{F}_q$:

Definition 5 *Suppose that $\theta \in Aut(\mathbb{F}_q)$ is defined by $a \mapsto a^{q_0}$ and that $q = {q_0}^r$. A skew BCH code of length n over $\mathbb{F}_q$ for the non zero positive integer parameters δ and s is a θ-code that is generated by a skew polynomial $g \in \mathbb{F}_q[X,\theta]$ with the property that*

1. *$g \in \mathbb{F}_q[X,\theta]$ is the skew polynomial of smallest degree that is right divisible by $X - \alpha^k$ for $k \in \{1,\ldots,\delta-1\}$ where α is a generator of the multiplicative group of $\mathbb{F}_{{q_0}^s}$.*

2. *g is bounded by a polynomial of degree n.*

We note such a code a (n, q_0, r, s, δ) skew BCH code.

The following is a generalization of [4], Proposition 2

Proposition 2 *If $n \leq (q_0 - 1)\cdot s$, then an (n, q_0, r, s, δ) skew BCH code has distance at least δ.*

Proof. Suppose that the code is generated by $g \in \mathbb{F}_q[X,\theta]$ and that f is a bound of degree n of g. An element $h = \sum_{i=0}^{n-1} c_iX^i \in \mathbb{F}_q[X,\theta]/(f)$ is a code word if and only if it is a left multiple of g, or equivalently, if α^k is a root of $\mathcal{P}_h(Y) \in \mathbb{F}_q[Y]$ for $k \in \{1,\ldots,\delta-1\}$.

We write $[i] = \frac{(q_0)^i - 1}{q_0 - 1}$ and like in the proof of ([4], Proposition 2) we obtain a parity-check matrix of the form

$$\begin{pmatrix} \alpha & \alpha^{[1]} & \cdots & \alpha^{[\delta-1]} & \cdots & \alpha^{[n-1]} \\ (\alpha^2) & (\alpha^2)^{[1]} & \cdots & (\alpha^2)^{[\delta-1]} & \cdots & (\alpha^2)^{[n-1]} \\ \vdots & & & & & \vdots \\ (\alpha^{\delta-1}) & (\alpha^{\delta-1})^{[1]} & \cdots & (\alpha^{\delta-1})^{[\delta-1]} & \cdots & (\alpha^{\delta-1})^{[n-1]} \end{pmatrix}.$$

The determinant of all extracted $(\delta - 1) \times (\delta - 1)$ is non zero if and only if $\alpha^{[i]} - \alpha^{[j]} \neq 0$ for $i > j$ in $\{0, 1, \ldots, n-1\}$. This follows from $\alpha^{[i]} = \alpha^{[j]}$ if and only if

$$\alpha^{\frac{(q_0)^i - (q_0)^j}{q_0 - 1}} = \alpha^{\frac{(q_0)^j \cdot \left((q_0)^{i-j} - 1\right)}{q_0 - 1}} = 1. \tag{5}$$

In particular $\alpha^{(q_0)^j \cdot \left((q_0)^{i-j} - 1\right)} = 1$, which implies that $(q_0)^{i-j} - 1$ is divisible by $(q_0)^s - 1$, the order of α. This shows that $i - j = m \cdot s$ and from relation (5), we now get that $q_0 - 1$ must divide

$$\frac{q_0^{m \cdot s} - 1}{q_0^s - 1} = \sum_{r=0}^{m-1} (q_0)^{s \cdot k}.$$

Therefore $q_0 - 1$ divides m, showing that $i - j$ is a multiple of $(q_0 - 1) \cdot s$. Since $i - j < n \leq (q_0 - 1) \cdot s$, this is impossible. ∎

Denote α a generator of the multiplicative group of $\mathbb{F}_{(q_0)^s}$. Note that g is right divisible by $X - \alpha^i$, if and only if the solution β_i of $\theta(y) - \alpha^i y = 0$, is a solution of the difference equation $L_g(y) = 0$ associated to g, i.e. $\theta(\beta_i)/\beta_i = \alpha^i$. The fact that $g \in \mathbb{F}_q[X, \theta]$ is the skew polynomial of smallest degree that is right divisible by $X - \alpha^k$ for $k \in \{1, \ldots, \delta - 1\}$ is therefore equivalent to the solution space V_g of $L_g(y) = 0$ containing $\beta_1, \beta_2, \ldots, \beta_{\delta-1}$. According to Lemma 2, for $L_g(y)$ (and therefore g) to be defined over $\mathbb{F}_q$, the vector space V_g must be stable under a generator σ of $\mathrm{Aut}(\mathbb{F}_{q_0^s}/\mathbb{F}_q)$. The following gives an algorithm to find (n, q_0, r, s, δ) skew BCH code with designed distance $\delta \geq \Delta$:

1. For each generator α of $(\mathbb{F}_q)^*$, compute β_i (where $i \in \{1, \ldots, \Delta - 1\}$) such that $\theta(\beta_i)/\beta_i = \alpha^i$.

2. Compute the smallest $\mathbb{F}_{q_0}$-vector space V_g that contains $\beta_1, \beta_2, \ldots, \beta_{\Delta-1}$ which is invariant under a generator σ of $\mathrm{Aut}(\mathbb{F}_{q_0^s}/\mathbb{F}_q)$.

3. Using the Casoratian determinant on a basis of V_g, Compute the skew polynomial $g \in \mathbb{F}_q[X, \theta]$ associated to the corresponding difference operator, having the solution space V_g.

4. Compute a bound $f \in \mathbb{F}_{q_0}[X^m]$ for g (here m denote the order of $\theta \in \mathrm{Aut}(\mathbb{F}_q)$. If the degree n of f is such that $n \leq (q_0 - 1) \cdot s$, then g will denote a skew BCH code of designed distance $\geq \Delta$.

5. In order to compute the real designed distance of the resulting code, we compute the largest integer δ with the property, that $\beta_1, \beta_2, \ldots, \beta_{\delta-1}$ are solutions of $L_g(y) = 0$.

In order to simplify the computation of the bound f of g, we can use the fact that the solution space of $f \in \mathbb{F}_{q_0}[X, \theta] \subset \mathbb{F}_{q_0}[X^m]$ must be invariant under $\Theta \in \mathrm{Aut}(\mathbb{F}_{q_0{}^s}/\mathbb{F}_{q_0})$ (Lemma 2). In particular the smallest $\mathbb{F}_{q_0}$-vector space V_F that contains V_g and is invariant under $\Theta \in \mathrm{Aut}(\mathbb{F}_{q_0{}^s}/\mathbb{F}_{q_0})$ will be included in the solution space V_f of $L_f(y) = 0$. If we denote $F \in \mathbb{F}_{q_0}[X, \theta] = \mathbb{F}_{q_0}[X]$ the skew polynomial associated to the difference equation whose solution space is V_F, this implies that f is (right) divisible by F in $\mathbb{F}_{q_0}[X, \theta] = \mathbb{F}_{q_0}[X]$. The computation of the bound f in the above procedure can therefore be replaced by :

1. Compute the smallest $\mathbb{F}_{q_0}$-vector space V_F that contains V_g and is invariant under $\Theta \in \mathrm{Aut}(\mathbb{F}_{q_0{}^s}/\mathbb{F}_{q_0})$ will be included in the solution space V_f of $L_f(y) = 0$.

2. Compute the skew polynomial $F \in \mathbb{F}_{q_0}[X, \theta] = \mathbb{F}_{q_0}[X]$ associated to the corresponding difference operator having the solution space V_F.

3. If the degree of F is t, then consider a polynomial $h \in \mathbb{F}_{q_0}[X]$ with unknown coefficients of degree $(q_0 - 1) \cdot s - t$. Verify if there are values in $\mathbb{F}_{q_0}$ for the unknown coefficients so that $h \cdot F$ belongs to $\mathbb{F}_{q_0}[X^m]$ for g (here m denotes the order of $\theta \in \mathrm{Aut}(\mathbb{F}_q)$. This leads to a system of linear equations over $\mathbb{F}_{q_0}$, which can be obtained by setting the corresponding coefficients of $h \cdot F$ to zero.

Example 6 *Consider* $\mathbb{F}_q = \mathbb{F}_{2^3}$, $\theta \colon x \mapsto x^2$ *and* $s = 9$. *This means that we will use elements* $\alpha \in \mathbb{F}_{2^9}$ *in order to construct codes over* $\mathbb{F}_{2^3}$. *We denote by* γ *the generator of* $\mathbb{F}_{2^9}$ *and by* w *the generator of* $\mathbb{F}_{2^3}$ *given by* MAGMA. *Consider* $\alpha = \gamma^{433}$ *and* $\delta = 2$. *The smallest* $\mathbb{F}_2 = (\mathbb{F}_{2^3})^\theta$*-space* V_{α,α^2} *containing* $\{\alpha, \alpha^2\}$ *which is stable under the generator* $\sigma \colon x \mapsto x^8$ *of* $Aut(\mathbb{F}_{2^9}/\mathbb{F}_3)$ *has a basis* $\{\alpha, \gamma^{483}, \gamma^{410}, \gamma^{179}\}$. *Using the Casoratian determinant, we compute*

$$L_{\alpha,\gamma^{483},\gamma^{410},\gamma^{179}}(y) = \theta^4(y) + w^2\theta^3(y) + w\theta^2(y) + w\theta(y) + y$$

The skew polynomial $g = X^4 + w^2X^3 + wX^2 + wX + 1 \in \mathbb{F}_{2^3}[X, \theta]$ *will be the generator of the skew code we are constructing. The bound of* g *is* $f = X^6 + X^3 + 1 \in \mathbb{F}_2[X^3]$. *Therefore the length of the skew code will be* 6 *and its generating matrix is*

$$\begin{pmatrix} 1 & w & w & w^2 & 1 & 0 \\ 0 & 1 & w^2 & w^2 & w^4 & 1 \end{pmatrix}$$

We obtain a $[6, 2, 5]$ *skew code over* $\mathbb{F}_8$ *of prescribed distance* 3.

The following tables show the characteristics of codes with prescribed distance that are defined over $\mathbb{F}_4$. The lines indicates the fields where α has been found and the column indicate the distance Δ that has been prescribed during the construction (the actual prescribed distance could be larger). The entry $[6, 3, 3](8)$ means that 8 different skew polynomials g

have been found for the values $[6, 3, 3]$. In the following table we can observe that prescribing a certain distance may result in a code with the same characteristics where a higher distance could have been prescribed.

	$\Delta = 2$	$\Delta = 3$	$\Delta = 4$	$\Delta = 5$	$\Delta = 6$	$\Delta = 7$
$\mathbb{F}_{2^6}$	$[6, 3, 3](6)$ $[6, 3, 4](6)$	$[6, 1, 6](1)$ $[6, 2, 4](1)$	$[6, 1, 6](1)$	$[6, 1, 6](1)$		
$\mathbb{F}_{2^8}$	$[8, 4, 4](20)$ $[6, 3, 3](8)$	$[8, 1, 8](1)$ $[6, 1, 4](1)$	$[8, 1, 8](3)$			
$\mathbb{F}_{2^{10}}$	$[10, 5, 4](24)$ $[10, 5, 5](24)$ $[\mathbf{10}, \mathbf{6}, \mathbf{3}](2)$ $[\mathbf{8}, \mathbf{4}, \mathbf{4}](12))$	$[10, 1, 10](1)$ $[10, 4, 4](1)$	$[10, 1, 10](3)$	$[10, 1, 10](3)$	$[10, 1, 10](3)$	$[10, 1, 10](3)$
$\mathbb{F}_{2^{12}}$	$[12, 6, 3](12)$ $[12, 6, 4](18)$ $[12, 6, 5](54)$ $[\mathbf{12}, \mathbf{6}, \mathbf{6}](12)$ $[12, 7, 3](6)$ $[\mathbf{12}, \mathbf{7}, \mathbf{4}](12)$ $[\mathbf{12}, \mathbf{8}, \mathbf{3}](6)$ $[10, 5, 3](6)$ $[\mathbf{10}, \mathbf{5}, \mathbf{4}](18)$ $[8, 4, 3](12)$ $[\mathbf{8}, \mathbf{4}, \mathbf{4}](18)$	$[\mathbf{12}, \mathbf{1}, \mathbf{12}](1)$ $[\mathbf{12}, \mathbf{2}, \mathbf{8}](1)$ $[\mathbf{12}, \mathbf{3}, \mathbf{4}](1)$ $[\mathbf{10}, \mathbf{1}, \mathbf{6}](1)$ $[10, 2, 4](1)$ $[\mathbf{10}, \mathbf{3}, \mathbf{4}](1)$ $[8, 1, 4](1)$ $[8, 2, 4](1)$ $[8, 2, 5](1)$ $[8, 3, 4](1)$	$[\mathbf{12}, \mathbf{1}, \mathbf{12}](3)$ $[12, 2, 6](2)$ $[12, 2, 8](3)$ $[\mathbf{12}, \mathbf{2}, \mathbf{9}](4)$ $[\mathbf{12}, \mathbf{4}, \mathbf{6}](2)$	$[\mathbf{12}, \mathbf{1}, \mathbf{12}](3)$ $[12, 2, 6](2)$ $[12, 2, 8](3)$ $[\mathbf{12}, \mathbf{2}, \mathbf{9}](3)$ $[\mathbf{12}, \mathbf{4}, \mathbf{6}](2)$	$[\mathbf{12}, \mathbf{1}, \mathbf{12}](3)$ $[12, 2, 8](1)$ $[\mathbf{12}, \mathbf{2}, \mathbf{9}](4)$	$[\mathbf{12}, \mathbf{1}, \mathbf{12}](3)$ $[\mathbf{12}, \mathbf{2}, \mathbf{8}](1)$
$\mathbb{F}_{2^{14}}$	$[14, 7, 4](24)$ $[14, 7, 5](84)$ $[\mathbf{14}, \mathbf{7}, \mathbf{6}](132)$ $[12, 6, 4](30)$ $[\mathbf{12}, \mathbf{6}, \mathbf{5}](48)$ $[8, 4, 3](24)$ $[\mathbf{8}, \mathbf{4}, \mathbf{4}](8)$ $[\mathbf{6}, \mathbf{3}, \mathbf{3}](8)$	$[14, 1, 14](1)$ $[14, 3, 8](2)$ $[14, 4, 6](2)$ $[14, 6, 4](1)$	$[\mathbf{14}, \mathbf{1}, \mathbf{14}](3)$ $[14, 3, 8](2)$ $[\mathbf{14}, \mathbf{3}, \mathbf{10}](4)$ $[14, 4, 6](2)$ $[\mathbf{14}, \mathbf{4}, \mathbf{8}](4)$	$[\mathbf{14}, \mathbf{1}, \mathbf{14}](3)$ $[14, 3, 8](2)$ $[\mathbf{14}, \mathbf{3}, \mathbf{10}](4)$ $[\mathbf{14}, \mathbf{4}, \mathbf{6}](2)$	$[14, 1, 14](3)$ $[14, 3, 8, 1]$	$[14, 1, 14](3)$ $[14, 3, 8](1)$

The following table, organized in the same way as the previous table, shows the characteristics of codes with prescribed distances that are defined over $\mathbb{F}_8$.

	$\Delta = 2$	$\Delta = 3$	$\Delta = 4$	$\Delta = 5$
$\mathbb{F}_{8^2}$	$[\mathbf{6},\mathbf{4},\mathbf{3}](18)$	$[\mathbf{6},\mathbf{2},\mathbf{5}](12)$ $[\mathbf{6},\mathbf{3},\mathbf{4}](3)$	$[\mathbf{6},\mathbf{2},\mathbf{5}](9)$ $[\mathbf{6},\mathbf{1},\mathbf{6}](3)$	$[\mathbf{6},\mathbf{1},\mathbf{6}](3)$
$\mathbb{F}_{8^3}$	$[9,6,3](108)$ $[\mathbf{9},\mathbf{6},\mathbf{4}](18)$ $[\mathbf{6},\mathbf{3},\mathbf{4}](18)$	$[9,3,6](60)$ $[\mathbf{9},\mathbf{3},\mathbf{7}](12)$ $[9,4,5](12)$ $[\mathbf{9},\mathbf{4},\mathbf{6}](3)$ $[\mathbf{6},\mathbf{2},\mathbf{5}](18)$	$[\mathbf{9},\mathbf{1},\mathbf{9}](6)$ $[9,2,6](6)$ $[\mathbf{9},\mathbf{2},\mathbf{8}](6)$ $[9,3,6](24)$ $[\mathbf{9},\mathbf{3},\mathbf{7}](3)$ $[\mathbf{9},\mathbf{4},\mathbf{5}](3)$	$[\mathbf{9},\mathbf{1},\mathbf{9}](3)$ $[\mathbf{9},\mathbf{2},\mathbf{6}](6)$
$\mathbb{F}_{8^4}$	$[12,8,3](132)$ $[\mathbf{12},\mathbf{8},\mathbf{4}](183)$ $[\mathbf{9},\mathbf{6},\mathbf{3}](54)$	$[12,4,5](12)$ $[12,4,6](60)$ $[\mathbf{12},\mathbf{4},\mathbf{7}](48)$ $[12,5,6](21)$ $[\mathbf{12},\mathbf{5},\mathbf{7}](12)$ $[12,6,4](12)$ $[\mathbf{12},\mathbf{7},\mathbf{4}](3)$ $[\mathbf{12},\mathbf{8},\mathbf{4}](72)$ $[9,3,5](12)$ $[\mathbf{9},\mathbf{3},\mathbf{6}](21)$ $[9,4,4](6)$ $[\mathbf{9},\mathbf{5},\mathbf{4}](3)$	$[\mathbf{12},\mathbf{1},\mathbf{12}](6)$ $[12,2,6](3)$ $[12,2,8](6)$ $[\mathbf{12},\mathbf{2},\mathbf{10}](9)$ $[12,3,6](6)$ $[12,3,8](3)$ $[\mathbf{12},\mathbf{3},\mathbf{9}](18)$ $[12,4,7](9)$ $[\mathbf{12},\mathbf{4},\mathbf{8}](3)$ $[12,5,5](3)$ $[\mathbf{12},\mathbf{5},\mathbf{6}](12)$ $[\mathbf{12},\mathbf{6},\mathbf{5}](3)$	$[\mathbf{12},\mathbf{1},\mathbf{12}](3)$ $[12,2,6](3)$ $[12,2,8](6)$ $[\mathbf{12},\mathbf{2},\mathbf{10}](3)$ $[12,3,6](9)$ $[12,3,8](6)$ $[\mathbf{12},\mathbf{3},\mathbf{9}](3)$ $[12,4,6](3)$ $[\mathbf{12},\mathbf{5},\mathbf{6}](3)$

4 Decoding skew BCH codes

These skew codes are built in analogy to BCH codes and it is possible to adapt the classical algorithm to decode these codes.

Using the notations of the definition 5, we consider a (n, q_0, r, s, δ) skew BCH code : $\mathcal{C}$. We assume that this code can correct t errors.
Consider the code word $c \in \mathcal{C}$ and the error $e(x) = e_{i_1}x^{i_1} + ... + e_{i_r}x^{i_r}$. We assume that $r \leq t$ and denote
$c' = c + e = \sum_{j=0}^{n} c'_j x^j$ the received word.

The question is how to find e knowing c'.

1) According to [8] theorem 1.3.11 we get that the remainder of the right division of e by $X - \alpha^i$ for $i = 1, ..., \delta - 1$ is

$$A_i = \sum_{j=0}^{n-1} e_j (\alpha^i)^{[j]}$$

where $\beta^{[j]} = \beta^{\frac{(q_0)^i - 1}{q_0 - 1}}$.

It is possible to compute A_i only with c' since the remainder of the right division of e by $X-\alpha^i$ is the same as the remainder of the right division of c' by $X-\alpha^i$ (since c is right divisible by $X-\alpha^i$).

Since A_i is also equal to $\sum_{j=0}^{n-1} c'_j(\alpha^i)^{[j]}$, it can be calculated only knowing c'.

One defines the syndrome polynomial of e as the polynomial :

$$S(z) = \sum_{k=1}^{\delta-1} A_i z^{i-1} \in \mathbb{F}_{q^s}[z]$$

2) One also defines the pseudo-locator polynomial :

$$\sigma(z) = \prod_{k=1}^{r}(1-\alpha^{[i_k]})$$

and the evaluator polynomial :

$$w(z) = \sum_{l=1}^{r} e_{i_l}\alpha^{[i_l]} \prod_{k\neq l}(1-\alpha^{[i_k]}z)$$

3) Knowing $\sigma(z)$ enables us to find the $[i_k] = \frac{(q_0)^{i_k}-1}{q_0-1} \bmod(q^s-1)$. To do that we have to find $[i_1],...[i_r]$ such as $\sigma(\alpha^{-[i_1]}) = ... = \sigma(\alpha^{-[i_r]}) = 0$, this research can be done by testing $\sigma(x)$ for all $x \in \mathbb{F}_{q^s}$.

Knowing $[i_k]$ and $w(z)$ enables us to find the coefficients e_{i_k} since

$$e_{i_k} = \alpha^{-[i_k]} w(\alpha^{-[i_k]}) \prod_{l\neq k}(1-\alpha^{[i_l]-[i_k]})$$

for $k \in \{1...r\}$.

4) We apply Euclid's algorithm to the polynomials $S(z)$ and $z^{\delta-1}$ in $\mathbb{F}_{q^s}[z]$, we stop as soon as we find the first remainder of degree less than t, then we have :

$$u(z)z^{\delta-1} + v(z)S(z) = r(z)$$

As in the classical BCH algorithm, we can prove that $\sigma(z) = v(z)/v(0)$ and $w(z) = r(z)/v(0)$. And if we know σ and w, we have seen that we can rebuild the error e and find the codeword c.

References

[1] McDonald, B.R., *Finite Rings with Identity.*, Marcel Dekker Inc. (1974).

[2] Bomboy, R. (1999), *Réductibilité des opérateurs aux différences finies: une approche Galois-théorique*, Rapport Inria 3735.

[3] Bosma,W., Cannon,J. and Playoust,C. (1997). The Magma Algebra System I: The User Language. *Journal of Symbolic Computation,* **24**, pp. 235–265.

[4] Boucher,D. , Geiselmann,W. and Ulmer, F. (2007), *Skew Cyclic Codes*, Applied Algebra in Engineering, Communication and Computing, Vol. 18, pp 379 - 389.

[5] Boucher,D. and Ulmer, F. (2007), *Coding with skew polynomial rings*, Prépublication IRMAR 08-07, to appear in *Journal of Symbolic Computation.*

[6] Bronstein,M. and Petkovsek,M. (1994), *On Ore Rings, Linear Operators and Factorisation*, Programming and Computer Software, **20**, pp. 14–26

[7] Gabidulin, E. M. and Kshevetskiy, A. (2005) The new construction of rank codes. *2005 IEEE International Symposium on Information Theory, ISIT'05*, pp. 2105 – 2108. –

[8] Gabidulin, E. M. (1985) Theory of codes with maximal rank distance. *Problems of Information Transmission*, vol. 21, pp. 1–12.

[9] Jacobson, N., *Finite dimentional algebras over division fields.*, Springer-Verlag. (1996).

[10] Lidl, R and Niederreiter, H. *Fnite Fields.*, Encyclopedia of Mathematics and its Applications Vol. 20, Amsterdam: Addison-Wesley. (1956).

[11] Lidl, R and Niederreiter, H. *Introduction to finite fields and their applications.*, Cambridge University Press. (1994).

[12] Ore, O. (1933). Theory of non-commutative polynomials. *Ann. of Math.* **34**.

[13] Ore, O. (1933). On a Special Class of Polynomials *Transactions of the American Mathematical Society*, Vol. 35, pp. 559-584

[14] Singer, M.F., Van der Put, Marius *Galois Theory of difference equations.*, Springer Lecture Notes in Mathematics, 1666. (1997).

[15] Singer, M.F., Van der Put, Marius *Galois Theory of linear differencial equations.*, Grundlehren der mathematischen Wissenschaften, Springer (2003).